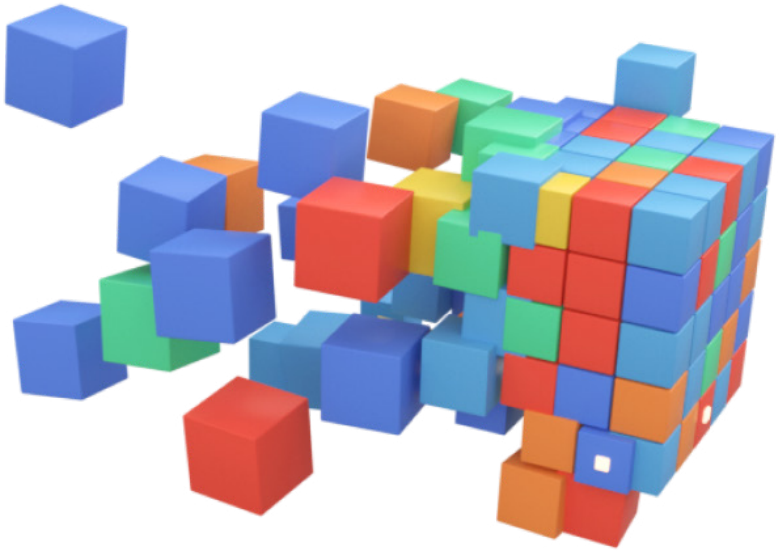
VULCAN™ | EBOOK

The Four Levels of Mature Vulnerability Remediation

Table of Contents

- Introduction
- The Vulnerability Remediation Orchestration Imperative
- What Is Remediation Orchestration?
- Introducing the Vulnerability Remediation Maturity Model
- Building for Company-Wide Transformation
- Level 2: Data-Driven Vulnerability Management
- Level 3: Orchestrating Remediation Across Tools and Teams
- Level 4: Achieving Cybersecurity Transformation
- Conclusion



Introduction

As IT environments become more complex, enterprises find themselves wrangling vulnerabilities at scale in diverse asset environments deployed across distributed architectures. In the old days, vulnerability management dealt primarily with servers and hosts running on bare metal in the company's data center. Today, vulnerability management has been extended to cloud-native environments with virtual machines running in every cloud, to code repositories and container images, and to storage and network infrastructure.

Further complicating matters is the fact that organizational structures have also become highly distributed to maintain a competitive edge in the modern economy. As a result, vulnerability remediation workflows span diverse teams (e.g., security, operations, product, development, and lines of business), each with its own business mandate, unique processes, and tech stack.

These combined with the fact that vulnerabilities and exploits are growing exponentially and the modern enterprise has a daunting challenge to ensure vulnerability management programs consistently achieve their principal business-critical outcome:

effective and timely vulnerability remediation that enhances a company's security posture while consuming minimal resources.

This eBook establishes the first vulnerability management maturity model to advance several levels beyond simple vulnerability scanning or prioritization. It outlines a comprehensive maturity model for full vulnerability remediation defining the mandate for organizations to drive vulnerability management programs to higher levels of maturity and analyzing the elements that comprise transformative, end-to-end vulnerability remediation.

A traditional vulnerability management program run by security teams to deliver prioritized vulnerabilities has been properly addressed by the industry and its practitioners. Collaborative, outcome-driven vulnerability remediation that results in cross-functional organizational efficiency and more secure IT environments remains uncharted territory for most. The latter is challenging, but achievable with fully utilized tools, willing people, and a mature process.

This vulnerability remediation maturity model establishes the industry's first end-to-end framework to help security and IT operations teams work together to achieve advanced levels of vulnerability management maturity. It explains why a company must have a strategic vision of vulnerability management outcomes in order to mature its program from a reactive level to data-driven → orchestrated → transformational. It describes how an organization must systematically optimize its vulnerability management processes at each level in order to move inexorably towards its ultimate goal: data-driven, well-orchestrated, and smart vulnerability remediation.

The Vulnerability Remediation Orchestration Imperative

The following trends are reshaping the vulnerability management landscape:

- **A growing number of vulnerabilities year over year.**
  According to an Imperva report, there were 20,362 new vulnerabilities in 2019. This figure represented an increase of 17.6% over 2018 and 44.5% over 2017.

- **Highly diverse vulnerabilities in all layers.**
  Prior to public cloud, vulnerabilities were associated primarily with server/host infrastructure and OS layers. Today, assets under management are far more diverse. They include online assets such as code repositories, cloud storage resources, container images, and more. An open S3 bucket, for example, exposes an organization as much as any vulnerability assigned a CVE # by the legacy vulnerability trackers.

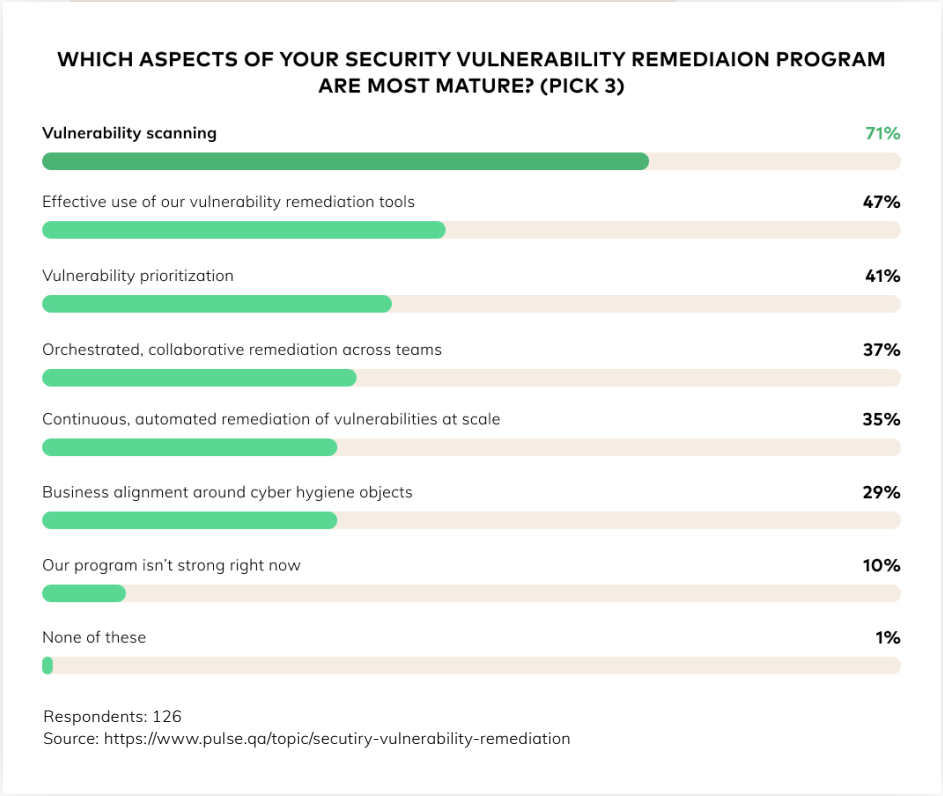
- **The inherent complexity and scope of the enterprise environment.**
  According to the RightScale (now Flexera) 2019 State of the Cloud Report, 58% of enterprises have embraced a hybrid strategy combining both public and private clouds, while 84% use multiple clouds. These complex environments comprise thousands of infrastructure assets running on a wide range of operating systems and versions. They deploy hundreds of applications and workloads, both on-premises and in the cloud. Numerous types of edge devices, from laptops to smartphones and IoT devices, now connect to corporate networks.

- **The general shortage in skilled cybersecurity personnel.**
  The cybersecurity unemployment rate is 0%, and, according to CSO Online, it is expected to stay there through 2021. In the meantime, ISSA reports that 82% of employers report a shortage of cybersecurity skills.

- **New development processes (and a new mindset).**
  Security teams must align themselves with the highly automated continuous development and continuous integration (CI/CD) development workflow of DevOps teams.

- **It's all about collaboration.**
  Many teams, each with their own goals, KPIs, and stacks, must work together to achieve effective vulnerability remediation. It is essential that enterprises close communication and collaboration gaps.

No doubt each of these data breaches were the result of a disconnect in the system. Teams that do not collaborate with teams. Tools that exist alone in a silo. Fragmented processes that are not outcome driven or that do not represent the full intent of a vulnerability management program. These program gaps are typically the root cause of the fall.



Take for example this data pulled from a survey of 120 security and IT executives commissioned by Vulcan Cyber.

Eighty two percent of respondents agree or strongly agree their vulnerability remediation program is mature. However, the vast majority of respondents also claim that vulnerability scanning is the most mature aspect of their vulnerability remediation program, which simply represents the first level of maturity. Perception of what is a mature vulnerability management program is significantly disconnected from the reality.

Today's vulnerability landscape requires organizations to manage many and diverse vulnerabilities—not all of which are tracked by legacy vulnerability scanning—with limited skilled resources distributed across multiple, often-siloed teams.

Legacy vulnerability management programs do not provide the focus, risk-based insights, and collaborative framework that are necessary for achieving vulnerability remediation outcomes optimized for a specific enterprise. Take the following hypothetical scenario:

- The typical enterprise manages about 50,000 assets, of which about 80% are servers and virtual machines, and the rest are a wide range of endpoints. It is also managing about 20 code repositories and the same number of public-facing websites.

- This enterprise will be facing at least 1,000 new vulnerability instances (the occurrence of a given vulnerability in the environment) *per week*.

- Even if the enterprise manages to prioritize high-risk vulnerabilities down to 5%, it is still facing thousands of vulnerability instances that need remediation, where a vulnerability instance is each asset that is affected by any given vulnerability. The remediation task is made even more difficult by non-orchestrated workflows that are primarily manual processes distributed across security, operations, development, and business unit teams—each with their own tools, responsibilities and priorities.

Vulnerability remediation orchestration and automation are essential to the effective management of today's formidable vulnerability landscape.

What Is Remediation Orchestration?

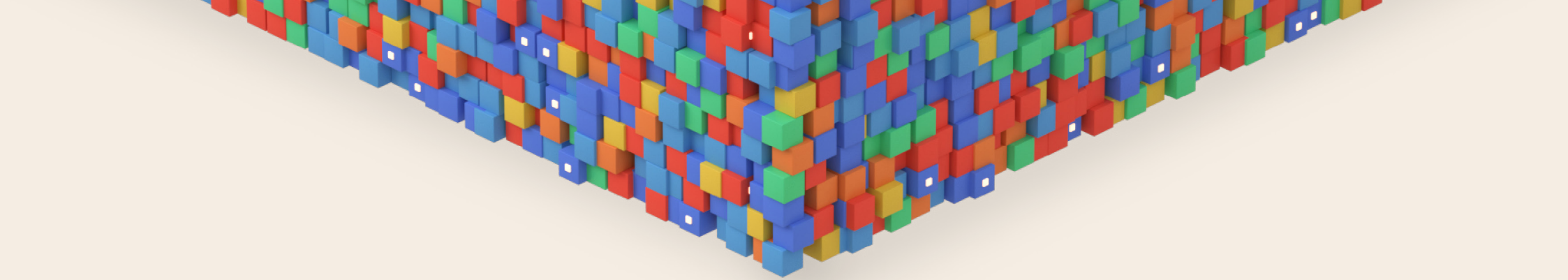
The Vulcan Cyber philosophy maintains vulnerability management programs must focus on the end game of achieving optimal vulnerability remediation outcomes. An effective vulnerability management program and its processes must be built strategically from the ground up with a constant eye on the desired outcome. This approach "reverse engineers" the outcome in which vulnerability management methodologies and tools are rethought in order to support true remediation orchestration in the modern enterprise environment.

This is the Vulcan Cyber remediation orchestration (RO) equation:

RO = RBVM + RI + RA

Where:

- **RBVM** (risk-based vulnerability management is a term coined by Gartner) means data-driven assessment and prioritization of vulnerabilities based not only on criticality scores, but also on the vulnerability's impact within a given organization's environment.
- **RI** (remediation intelligence) is a solution-focused stream of vulnerability knowledge.
- **RA** (remediation automation) refers to intelligence-based remediation workflows that are as automated as possible and well-orchestrated across diverse teams and tool stacks.



Each half of the equation is essential for a remediation outcome. RBVM is not just external threat intelligence applied to unique vulnerabilities one at a time. RBVM must look at the level of “vulnerability instances” (specific vulnerabilities found on specific assets) within the organization, with sufficient context and flexibility to address the specific risks of the enterprise. When done right, RBVM enhances vulnerability assessment and prioritization in general and dramatically reduces the number of high-risk vulnerabilities requiring remediation.

At the heart of RO, typically positioned between RBVM and RA, is remediation intelligence (RI). RI consists of a solution-focused stream of vulnerability knowledge that tracks external and internal vulnerability intelligence:

- Remedies in the form of workarounds, configuration blueprints, compensating controls, vendor patches or other solutions provided by the technology vendor or the community.
- Threat vectors or real-time methods used to exploit vulnerabilities in the wild.
- Asset data collected from asset inventories such as CMDBs, cloud infrastructures, and management systems.
- Vulnerability exposure data collected from different security assessment scanners.

RI bridges the traditional gaps in a vulnerability management program to promote successful remediation outcomes for the entire organization. These gaps typically exist between steps in the remediation workflow which most often transverse teams and tools. A mature process accounts for gaps and blockers, and provides a well-orchestrated view of:

- The vulnerability itself, including which systems and versions it applies to, and its externally defined level of criticality.
- The assets (vulnerability instances) that it applies to within the organization, as well as the criticality of the vulnerability within the organization's specific business context.
- Relevant remedies and solutions for the vulnerability, including patches (and their versions), compensating controls, and configuration blueprints, and workarounds.
- The remediation automation tools and teams who make up the last-mile of the process and often automate the generation of change tickets in a tool like ServiceNow or Jira and then trigger remediation scripts and playbooks within an appropriate configuration automation or patch management platform such as Ansible, Chef, Ivanti, or SCCM.

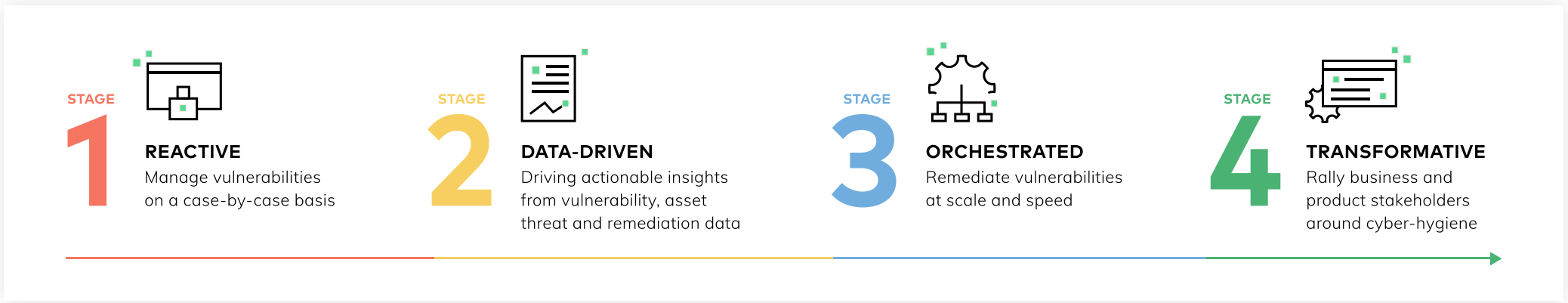
The role of RA is to provide an efficient framework within which teams can collaborate to achieve vulnerability remediation success. In particular, mature RA generates recommended remediation solutions and leverages the existing tools and inherent skills of the other vulnerability stakeholders (IT, DevOps, business units, and so on). The RA platform must integrate with all of the different stacks and provide a single source of remediation truth for the entire organization.

Effective RO requires both halves of the equation be in place, with each one multiplying the impact of the other.

True remediation orchestration is also on the mindset that vulnerability remediation is not a problem for the security team alone. Modern RO views the security team as enablers who support the execution decisions and activities of IT operations, DevOps, and engineering teams. Security teams must embrace the other stakeholders as allies, empowering them with solutions, remedies, and intelligence to make smart remediation decisions that balance security requirements with IT team-specific mandates and responsibilities.

The Four Levels of Mature Vulnerability Remediation

Introducing the Vulnerability Remediation Maturity Model



Based on our analysis of hundreds of enterprise vulnerability management program assessments and our experience with dozens of customers building their vulnerability remediation practice on the Vulcan platform, we have developed the Vulnerability Remediation Maturity Model (VRMM) to describe the enterprise journey from basic vulnerability management to a transformative program that delivers significant business value and peace of mind.

LEVEL 1

Reactive Vulnerability Scanning

The vast majority of organizations are at Level 1. As the poll above suggests, while the majority of participants trust their vulnerability scanning capabilities, when it comes to deriving insights or actionable steps from these scan results, most programs come short. In many cases, each team works in its own silo, juggling its own fragmented scanning and management stack. For example, the security team manages a collection of technology-specific scanners for its cloud infrastructure, on-premises infrastructure, static code, open-source code, and so on. Each tool looks for specific types of vulnerabilities and operates within its own unique frame of reference including risk management, false positive rates, and urgency levels. There is often a lot of duplication across the different scanners.

At this maturity level, an enterprise's vulnerability management program is tactical. With no cross-organizational visibility across workflows and policies, effective risk-based vulnerability triage is close to impossible. As a result, vulnerabilities are assessed on a case-by-case basis, and remediation is reactive.

LEVEL 2

Data-Driven Vulnerability Management

In Level 2, the enterprise security team and its allies have learned to normalize the diverse scanner outputs and enrich them with other internal and external data streams in order to derive actionable, prioritized vulnerability insights. The security team's data-driven, strategic vulnerability decisions are now based on a real-time understanding of asset status and criticality, compliance requirements, and threat intelligence.

LEVEL 3

Orchestrated Vulnerability Remediation

In Level 3, all of the vulnerability remediation stakeholders (security, IT operations, engineering, business unit owners) exit their silos. Their processes and practices become visible and their separate tech stacks are integrated into an orchestrated platform so that they can collaborate across fluid, optimized, and automated remediation workflows.

LEVEL 4

Transformative Cyber Hygiene

Level 4 can be considered the "holy grail" of a mature vulnerability management program. Transformative vulnerability remediation unites multiple cross-functional teams and organizational processes in a distributed framework in which non-security teams are empowered to take responsibility for vulnerability remediation decisions. As the undisputed governing entity in extremely high risk scenarios, security may override its allies' decisions. For the most part, however, vulnerability management at this stage is a democratized process in which stakeholders are given the tools, remedies and intelligent insight to independently make smart and correct vulnerability remediation decisions about the cyber hygiene of the enterprise.

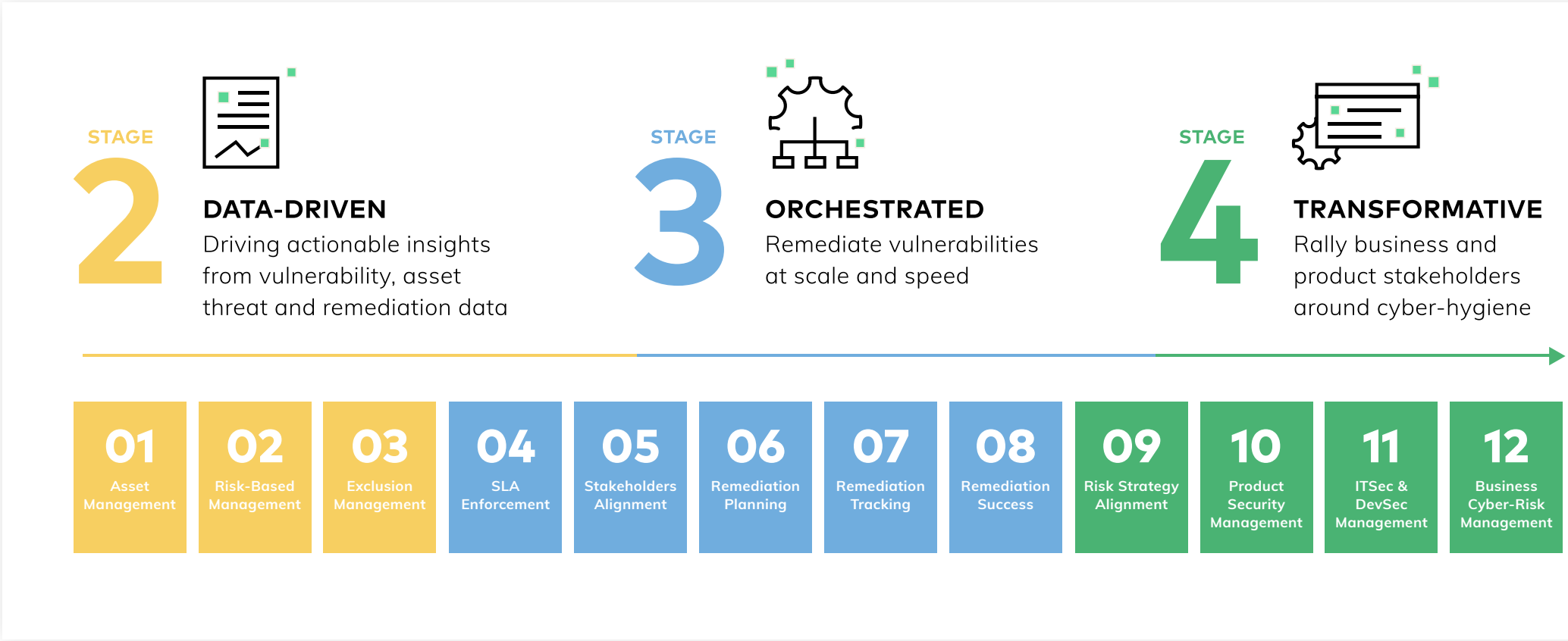
Building for Company-Wide Transformation

An enterprise's journey towards transformative, value-capturing vulnerability management consists of a series of milestones, with each achieved milestone setting the stage for the next leg of the journey.

The very first milestone is acknowledging the inherent conflict that exists between security and operations teams. The security team is responsible for scanning and for delegating remediation tasks to the operations team. The IT operations and DevOps teams are responsible for most of the actual remediation.

Each team is typically evaluated by different KPIs. The security team is measured by vulnerability management outcomes. If there is a security breach, it is the security team that will be held accountable. The operations team, on the other hand, is measured by infrastructure uptime, availability, and reliability. If business continuity is disrupted by a remediation task, such as deploying a patch, the operations team will be held accountable. Finally, the DevOps team is focused on adding business value in very short cycles. If their rapid development and deployment pipelines are slowed down by having to go back and fix bugs or secure code, they have a difficult time achieving their mandate.

In essence, the vulnerability remediation maturity model is a step-by-step strategic blueprint for closing the human, technological, process and operational gaps created when vulnerability remediation takes place across siloed teams. As shown in the figure below, each level consists of several foundations that represent the key outcomes to be achieved. Although the model maps a clear pathway toward vulnerability remediation, the process does not have to be strictly linear. The organization gains immediate and quantifiable vulnerability remediation benefits as it optimizes foundations at all different maturity levels. As mandate owners, the security team gains incremental tool, process and team buy-in to actually deliver cyber hygiene but only by working with engaged and empowered DevOps, IT operations, and business unit teams in seamless, collaborative vulnerability remediation workflows.



The following sections of this paper describe the vulnerability remediation foundations for each level within the Vulcan Vulnerability Remediation Maturity Model.

Building for Company-Wide Transformation

DATA-DRIVEN

There are three key foundations for the security team to optimize at the Data-Driven vulnerability management maturity level:

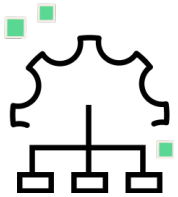
- **Asset Management**. The enterprise maps and maintains the status and risk attributes of every asset specific to the business (hosts, servers, cloud compute and storage, code repositories, and so on) and ensures that all assets are being scanned and managed for vulnerabilities.

- **Risk-Based Vulnerability Management.** Vulnerabilities are prioritized based on information provided by multiple disciplines, including threat intelligence, asset configuration data, available vendor solutions, and an understanding of the business impact of each possible remediation workflow. Risk algorithms should be customizable to the business for maximum efficiencies.

- **Compliance Management.** The ability of teams to choose security policies and compliance inputs to help focus on vulnerabilities and assets to look after and which to leave alone.

As these foundations undergo optimization, the enterprise benefits from data-driven vulnerability assessment and prioritization that takes into account the organization's unique asset, infrastructure, compliance, and business requirements. The security team can confidently identify the vulnerabilities that are truly high risk for the specific enterprise and pass on a dramatically smaller subset of high-priority vulnerabilities for remediation execution. Further, the organization can now take a strategic approach to its remediation campaigns, deciding when to be vulnerability-driven (solving a single vulnerability across all assets), when to be asset-driven (remediating all vulnerabilities affecting assets that impact the organization's security posture), and when to be solution-driven (patching an OS across the entire.

Level 3: Orchestrating Remediation Across Tools and Teams



ORCHESTRATED

04	05	06	07	08
SLA Enforcement	Stakeholders Alignment	Remediation Planning	Remediation Tracking	Remediation Success

At this level, the enterprise's remediation efforts go beyond the security team and establish a cross-organizational remediation workflow. The key foundations to be optimized at this level are:

- **SLA Enforcement.** Establish how quickly different vulnerabilities need to be addressed by different teams, product lines, environments, asset groups, and type of problems.
- **Stakeholders' Alignment.** Align the different remediation stakeholders (security, IT operations, DevOps, business unit owners, etc.) as to how they fit into and operate within the enterprise's chosen vulnerability remediation framework.
- **Remediation Planning.** Continuously design and implement effective remediation processes that are as automated as possible. Build and maintain playbooks that leverage data-driven recommendations and task statuses as triggers to drive workflows forward.
- **Remediation Tracking.** Ensure that all stakeholders can track the remediation workflows across teams, tools, and diverse processes.
- **Remediation Success.** At the task and workflow levels, define clear success criteria that can be used to verify that the remediation campaign effectively closed the detected vulnerability gaps.

When the enterprise has optimized its remediation orchestration framework, cybersecurity hygiene will be better upheld because vulnerability remediation is now far less disruptive to the IT operations, DevOps, and business teams. In addition, the overhead of manual work drops dramatically at this level. Non-security stakeholders are empowered to make responsible vulnerability remediation decisions within the framework of their unique mandates and responsibilities. And, the remediation workflows themselves are clear, transparent, and as seamless as they can possibly be.

Level 4: Achieving Cybersecurity Transformation

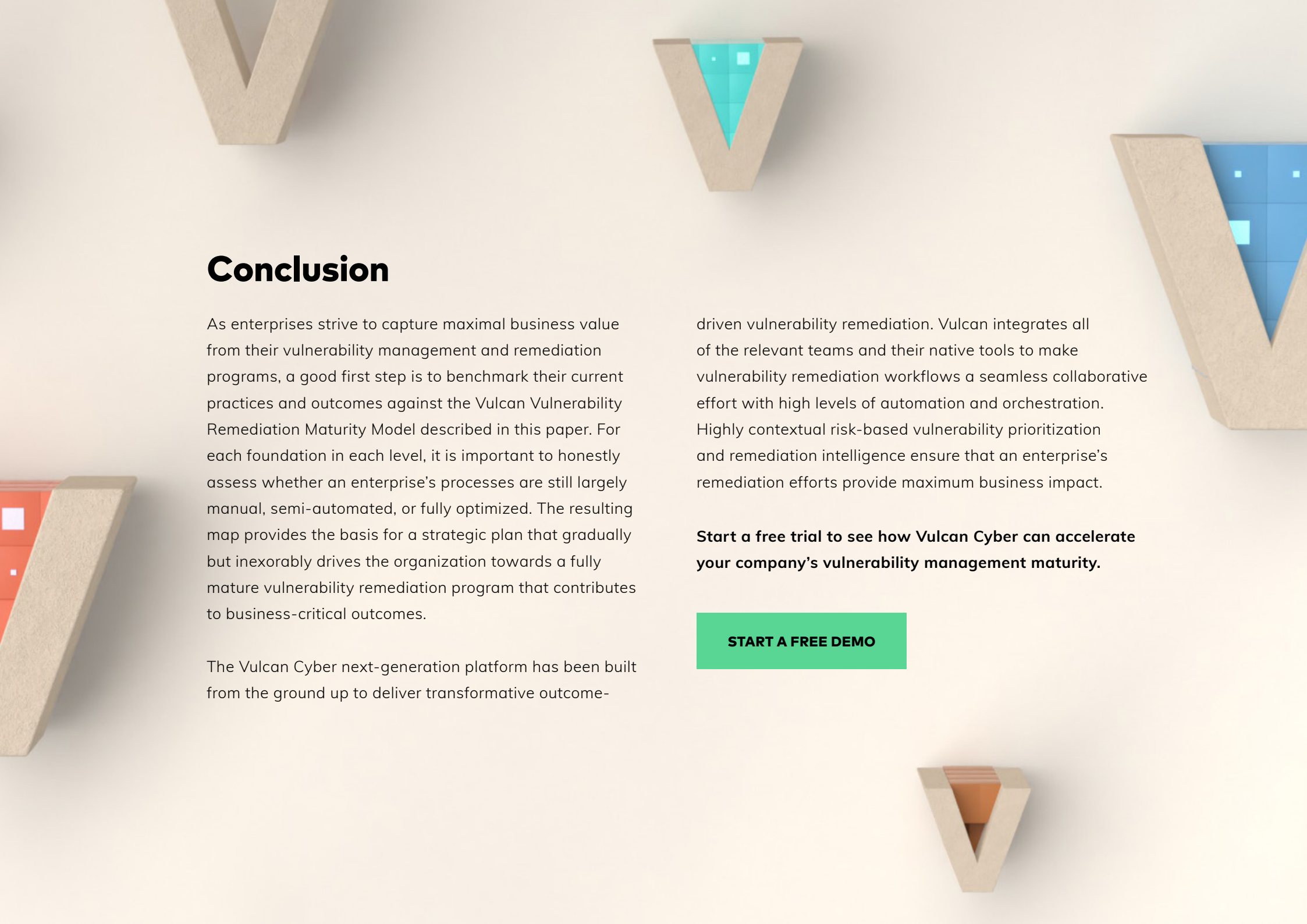
TRANSFORMATIVE

09	10	11	12
Risk Strategy Alignment	Product Security Management	ITSec & DevSec Management	Business Cyber-Risk Management

Now that the enterprise's vulnerability management program is data-driven and orchestrated, it can proceed to the transformative maturity level in which management functions within the organization can make informed cybersecurity decisions.

- **Risk Strategy Alignment.** The C-suite and board have access to user-friendly vulnerability management reports and dashboards that help them make decisions about where to invest resources in order to improve the organization's cybersecurity outcomes.
- **Product Security Management.** Product management teams can insightfully align their roadmaps with high priority security issues.
- **ITSec & DevSec Management.** Understand the tools and processes required to empower IT and development engineers to make smart remediation decisions.
- **Business Cyber-Risk Management.** Business unit owners receive dynamic tools that let them quickly understand their cyber-risk profile and compare their security performance with their peers', both within and outside of the organization.

At this transformative maturity level, security teams provide their allies with reports, dashboards, and insights that align with their native work environments and business vocabularies, empowering them to make smart decisions independently. Organizations leverage real-time insights into their vulnerability management program in order to make informed decisions about investments in vulnerability remediation tools, skills, policies, and processes that will further enhance business outcomes.



Conclusion

As enterprises strive to capture maximal business value from their vulnerability management and remediation programs, a good first step is to benchmark their current practices and outcomes against the Vulcan Vulnerability Remediation Maturity Model described in this paper. For each foundation in each level, it is important to honestly assess whether an enterprise's processes are still largely manual, semi-automated, or fully optimized. The resulting map provides the basis for a strategic plan that gradually but inexorably drives the organization towards a fully mature vulnerability remediation program that contributes to business-critical outcomes.

The Vulcan Cyber next-generation platform has been built from the ground up to deliver transformative outcome-driven vulnerability remediation. Vulcan integrates all of the relevant teams and their native tools to make vulnerability remediation workflows a seamless collaborative effort with high levels of automation and orchestration. Highly contextual risk-based vulnerability prioritization and remediation intelligence ensure that an enterprise's remediation efforts provide maximum business impact.

Start a free trial to see how Vulcan Cyber can accelerate your company's vulnerability management maturity.

START A FREE DEMO